WHAT IS CLAIMED IS:

1. A cryptographic system in a computer system, said cryptographic system comprising:

at least one server;

a database, said database constructed and arranged to contain sensitive information, said database responsive to signals from one of said at least one server;

enterprise credentials stored in said database;

a key repository process on one of said at least one server, said key repository having at least one master key, said at least one master key being constructed and arranged to manage information in said database, said key repository further constructed and arranged to authorize access to said sensitive information in said database, said key repository further constructed and arranged to access said enterprise credentials; and

at least one application on at least one of said at least one server;

wherein said key repository is enabled to record in said database those said applications that are authorized to obtain said enterprise credentials.

2. A cryptographic system as in claim 1, wherein said at least one master key protects said sensitive information in said database.

3. A cryptographic system as in claim 1, wherein said at least one master key provides privacy protection to said sensitive information on said database.

4. A cryptographic system as in claim 1, wherein said sensitive information is a public key.

5. A cryptographic system as in claim 1, wherein said sensitive information is a secret.

6. A cryptographic system as in claim 1, wherein said sensitive information is a private key.

7. A cryptographic system as in claim 1, wherein said sensitive information is a symmetric key.

8. A cryptographic system as in claim 1, wherein said sensitive information is a certification authority certificate.

9. A cryptographic system as in claim 1, wherein said keys are kept in physical memory.

10. A cryptographic system as in claim 1, wherein said keys are kept in non-swappable physical memory.

11. A cryptographic system as in claim 10, wherein said non-swappable physical memory is protected.

12. A cryptographic system as in claim 1, wherein said keys are kept in virtual memory.

13. A cryptographic system as in claim 1, wherein said key repository stores an integrity key, said integrity key constructed and arranged to ensure the integrity of said sensitive information on said database.

14. A cryptographic system as in claim 1, wherein said key repository stores a protection key, said protection key constructed and arranged to protect said sensitive information on said database.

15. A cryptographic system in a computer system, said cryptographic system comprising:

at least one server;

a database, said database constructed and arranged to contain sensitive information, said database responsive to signals from one of said at least one server;

enterprise credentials stored in said database;

at least one application process on said at least one server; and

a key repository process on said at least one server, said key repository having at least one master key, said at least one master key being constructed and arranged to manage said information in said database, said key repository further constructed and arranged to store in said database the identity of those said at least one applications that are authorized to access said enterprise credentials, said key repository further constructed and arranged to permit access to said enterprise credentials by said at least one application;

wherein if said at least one application is authorized to access said enterprise credentials, then transmitting said enterprise credentials from said key repository to said at least one application.

16. A cryptographic system in a computer system, said cryptographic system comprising:

at least one server;

a database, said database constructed and arranged to contain sensitive information, said database responsive to signals from one of said at least one server;

sensitive secrets stored in said database;

at least one application process on said at least one server; and

a key repository process on said at least one server, said key repository having at least one master key, said at least one master key being constructed and arranged to manage said information in said database, said key repository further constructed and arranged to store in said database the identity of those said at least one applications that are authorized to access said sensitive secrets said key repository further constructed and arranged to permit access to said sensitive secrets by said at least one application; and

wherein if said at least one application is authorized to access said sensitive secrets, then said key repository transmits said sensitive secrets to said at least one application.

17. A cryptographic system as in claim 16, wherein said at least one master key protects said sensitive information in said database from modification.

18. A cryptographic system as in claim 16, wherein said at least one master key provides privacy protection to said sensitive information in said database.

19. A cryptographic system as in claim 16, wherein said at least one of master key protects said sensitive information in said database from unauthorized deletion.

20. A cryptographic system as in claim 16, wherein said sensitive secret is a public key.

21. A cryptographic system as in claim 16, wherein said sensitive secret is a private key.

22. A cryptographic system as in claim 16, wherein said sensitive secret is a symmetric key.

23. A cryptographic system as in claim 16, wherein said sensitive secret is a trust root.

24. A cryptographic system as in claim 23, wherein said trust root is a digital fingerprint.

25. A cryptographic system as in claim 23, wherein said trust root is a checksum.

26. A cryptographic system as in claim 23, wherein said trust root is a hash.

27. A cryptographic system as in claim 23, wherein said trust root is a cryptographic mechanism.

28. A cryptographic system as in claim 16, wherein said keys are kept in physical memory.

29. A cryptographic system as in claim 16, wherein said keys are kept in non-swappable physical memory.

30. A cryptographic system as in claim 16, wherein said non-swappable physical memory is protected.

31. A cryptographic system as in claim 16, wherein said keys are kept in virtual memory.

32. A method of authorizing access to sensitive secrets on a computer system, said computer system having a server, an application, a database on said server, sensitive secrets on said server, and a key repository having at least one master key to manage said sensitive secrets on said database, said method comprising the steps of:

(a) storing authorization information in said database that is accessible by said key repository;

(b) querying said key repository by said application for access to said sensitive secrets;

(c) determining if said application is authorized to access said sensitive secrets by querying said authorization information in said database; and

(d) if said application is authorized to access said sensitive secrets, then transmitting said sensitive secrets from said key repository to said application;

wherein said application can invoke cryptographic resources on said server.

33. The method of claim 32, said method further comprising, before said step b), directing said key repository to recognize instances of said application.

34. The method of claim 32, wherein said key repository is constructed and arranged to record said authorization information in said database.

35. The method of claim 32, wherein a first of said two master keys protects said sensitive secrets from modification.

36. The method of claim 32, wherein a second of said two master keys provides privacy protection of said sensitive secrets on said database.

37. The method of claim 32, wherein at least one of said sensitive secrets is a public key.

38. The method of claim 32, wherein at least one of said sensitive secrets is a private key.

39. The method of claim 32, wherein at least one of said sensitive secrets is a symmetric key.

40. The method of claim 32, wherein at least one of said sensitive secrets is a trust root.

41. The method of claim 32, wherein at least one of said sensitive secrets is a digital fingerprint.

42. The method of claim 32, wherein at least one of said sensitive secrets is a digital signature.

43. The method of claim 32, wherein at least one of said sensitive secrets is a digital certificate.

44. The method of claim 32, wherein at least one of said sensitive secrets is a checksum.

45. The method of claim 32, wherein at least one of said sensitive secrets is a hash.

46. The method of claim 32, wherein at least one of said sensitive secrets is a characteristic code sequence.

47. The method of claim 32, wherein said master keys are kept in physical memory.

48. The method of claim 32, wherein said master keys are kept in non-swappable physical memory.

49. The method of claim 48, wherein said non-swappable memory is protected.

50. The method of claim 32, wherein said master keys are stored in virtual memory.

51. The method of claim 32, wherein said at least one master key is an integrity key, said integrity key being constructed and arranged to ensure the integrity of said sensitive secrets on said database.

52. The method of claim 32, wherein said at least one master key is a protection key, said protection key being constructed and arranged to protect said sensitive secrets on said database.

53. The method of claim 33, wherein said instance of said application is recognized by use of a cryptographic technique.

54. The method of claim 53, wherein said cryptographic technique is a checksum.

55. The method of claim 33, wherein said instance of said application is recognized by its file location.

56. The method of claim 33, wherein said instance of said application is recognized by its physical address.

57. The method of claim 33, wherein said instance of said application is recognized by the system on which it is instantiated.

58. The method of claim 33, wherein said instance of said application is recognized by the nature of the interconnection to said key repository.

59. The method of claim 33, wherein said instance of said application is recognized by its communication protocol.

60. The method of claim 33, wherein said instance of said application is recognized by a packet header.

61. The method of claim 32, wherein said authorization information includes a time constraint.

62. The method of claim 32, wherein said authorization information includes a file location.

63. The method of claim 32, wherein said authorization information includes a physical address.

64. The method of claim 32, wherein said authorization information includes a universal resource locator.

65. The method of claim 32, wherein said authorization information includes a system residence.

66. The method of claim 32, wherein said directive to authorize said application is provided by an operator.

67. The method of claim 32, wherein said directive to authorize said application is provided by an owner.

68. The method of claim 32, wherein said directive to authorize said application is provided by two or more owners.

69. The method of claim 32, wherein said directive to authorize said application is provided by two or more owners and an operator.